npj | Quantum Information

www.nature.com/npjqi

ARTICLE OPEN

Check for updates

Environment-assisted bosonic quantum communications

Stefano Pirandola[1]✉, Carlo Ottaviani[1], Christian S. Jacobsen[2], Gaetana Spedalieri[1], Samuel L. Braunstein[1], Tobias Gehring[2] and Ulrik L. Andersen[2]

We consider a quantum relay that is used by two parties to perform several continuous-variable protocols of quantum communication, from entanglement distribution (swapping and distillation) to quantum teleportation, and quantum key distribution. The theory of these protocols is suitably extended to a non-Markovian model of decoherence characterized by correlated Gaussian noise in the bosonic environment. In the worst-case scenario where bipartite entanglement is completely lost at the relay, we show that the various protocols can be reactivated by the assistance of classical (separable) correlations in the environment. In fact, above a critical amount, these correlations are able to guarantee the distribution of a weaker form of entanglement (quadripartite), which can be localized by the relay into a stronger form (bipartite) that is exploitable by the parties. Our findings are confirmed by a proof-of-principle experiment where we show, for the first time, that memory effects in the environment can drastically enhance the performance of a quantum relay, well beyond the single-repeater bound for quantum and private communications.

npj Quantum Information (2021)7:77 ; https://doi.org/10.1038/s41534-021-00413-2

INTRODUCTION

The concept of a relay is at the basis of network information theory[1]. Indeed the simplest network topology is composed by three nodes: two end-users, Alice and Bob, plus a third party, the relay, which assists their communication. This scenario is inherited by quantum information theory[2–13], where the mediation of a quantum relay can be found in a series of fundamental protocols. By sending quantum systems to a middle relay, Alice and Bob may perform entanglement swapping[14–17], entanglement distillation[18], quantum teleportation[19–21] and quantum key distribution (QKD)[22–27].

Quantum relays are crucial elements for quantum network architectures at any scale, from short-range implementations on quantum chips to long-distance quantum communication. In all cases, their working mechanism has been studied assuming Markovian decoherence models, where the errors are independent and identically distributed (iid). Removing this iid approximation is one of the goals of modern quantum information theory.

In a quantum chip (e.g., photonic[28,29] or superconducting[30]), quantum relays can distribute entanglement among registers and teleport quantum gates. Miniaturizing this architecture, correlated errors may come from unwanted interactions between quantum systems. A common bath may be introduced by a variety of imperfections, e.g., due to diffraction or slow electronics. It is important to realize that non-Markovian dynamics[31] will become increasingly important as the size of quantum chips further shrinks.

At long distances (in free-space or fibre), quantum relays intervene to assist quantum communication, entanglement and key distribution. Here, noise correlations and memory effects may naturally arise when optical modes are employed in high-speed communications[32], or propagate through atmospheric turbulence[33–35] and diffraction-limited linear systems. Most importantly, correlated errors must be considered in relay-based QKD, where an eavesdropper (Eve) may jointly attack the two links with the relay (random permutations and de Finetti arguments[36,37] cannot remove these residual correlations). Eve can manipulate the relay itself as assumed in measurement-device independent QKD[22–24]. Furthermore, Alice's and Bob's setups may also be subject to correlated side-channel attacks.

For all these reasons, we generalize the study of quantum relays to non-Markovian conditions, developing the theory for continuous-variable (CV) systems[10] (qubits are discussed in the Supplementary Material). We consider an environment whose Gaussian noise may be correlated between the two links. Our model is formulated as a spatial non-Markovian model, where spatially separated bosonic modes are subject to correlated errors, but could also be connected to a time-like model where the parties use the same channel at different times. In this scenario, while the relay always performs the same measurement, the parties may implement different protocols (swapping, distillation, teleportation, or QKD) all based, directly or indirectly, on the exploitation of bipartite entanglement.

We find a surprising behaviour in conditions of extreme decoherence. We consider entanglement-breaking links[38,39], so that no protocol can work under Markovian conditions. We then induce non-Markovian effects by progressively increasing the noise correlations in the environment while keeping their nature separable (so that there is no external reservoir of entanglement). While these correlations are not able to re-establish bipartite entanglement (or tripartite entanglement) we find that a critical amount reactivates quadripartite entanglement, between the setups and the modes transmitted. In other words, by increasing the separable correlations above a 'reactivation threshold' we can retrieve the otherwise lost quadripartite entanglement (it is in this sense that we talk of 'reactivated' entanglement below). The measurement of the relay can then localize this multipartite entanglement into a bipartite form, shared by the two remote parties and exploitable for the various protocols.

As a matter of fact, we find that all the quantum protocols can be reactivated. In particular, their reactivation occurs in a

[1]Department of Computer Science, University of York, York, UK. [2]Department of Physics, Technical University of Denmark, Kongens Lyngby, Denmark. ✉email: stefano.pirandola@york.ac.uk

progressive fashion, so that increasing the environmental correlations first reactivates entanglement swapping and teleportation, then entanglement distillation and finally QKD. Our theory is confirmed by a proof-of-principle experiment which shows the reactivation of the most nested protocol, i.e., the QKD protocol. In particular, we show that the key rate of this environmental-assisted protocol outperforms the single-repeater upper-bound for private communication[40], i.e., the maximum secret-key rate that is achievable in the presence of memoryless links.

RESULTS

General scenario

As depicted in Fig. 1, we consider two parties, Alice and Bob, whose devices are connected to a quantum relay, Charlie, with the aim of implementing a CV protocol (swapping, distillation, teleportation or QKD). The connection is established by sending two modes, A and B, through a joint quantum channel $\mathcal{E}_{AB}$, whose outputs A' and B' are subject to a CV Bell detection[41]. This means that modes A' and B' are mixed at a balanced beam splitter and then homodyned, one in the position quadrature $\hat{q}_- = (\hat{q}_{A'} - \hat{q}_{B'})/\sqrt{2}$ and the other in the momentum quadrature $\hat{p}_+ = (\hat{p}_{A'} + \hat{p}_{B'})/\sqrt{2}$. The classical outcomes q_- and p_+ can be combined into a complex variable $\gamma := q_- + ip_+$, which is broadcast to Alice and Bob through a classical public channel.

The joint quantum channel $\mathcal{E}_{AB}$ corresponds to an environment with correlated Gaussian noise. This is modelled by two beam splitters (with transmissivity $0 < \tau < 1$) mixing modes A and B with two ancillary modes, E_1 and E_2, respectively (see Fig. 1). These ancillas are taken in a zero-mean Gaussian state[10] $\rho_{E_1E_2}$ with covariance matrix (CM) in the symmetric normal form

$$\mathbf{V}_{E_1E_2}(\omega, g, g') = \begin{pmatrix} \omega\mathbf{I} & \mathbf{G} \\ \mathbf{G} & \omega\mathbf{I} \end{pmatrix}, \quad \begin{matrix} \mathbf{I} := \mathrm{diag}(1,1), \\ \mathbf{G} := \mathrm{diag}(g, g'). \end{matrix}$$

Here $\omega \geq 1$ is the variance of local thermal noise, while the block $\mathbf{G}$ accounts for noise correlations.

For $\mathbf{G} = \mathbf{0}$ we retrieve the standard Markovian case, based on two independent lossy channels[15–17]. For $\mathbf{G} \neq \mathbf{0}$, the lossy channels become correlated and the local dynamics cannot reproduce the global non-Markovian evolution of the system. Such a separation becomes more evident by increasing the correlation parameters, g and g', whose values are bounded by the bona fide conditions $|g| < \omega$, $|g'| < \omega$, and $\omega|g + g'| \leq \omega^2 + gg' - 1$ (refs. [42,43]). In particular, we consider the realistic case of separable environments ($\rho_{E_1E_2}$ separable), identified by the additional constraint $\omega|g - g'| \leq \omega^2 - gg' - 1$ (ref. [43]). The amount of separable correlations can be quantified by the quantum mutual information $I(g, g')$.

To analyse entanglement breaking, assume the asymptotic infinite-energy scenario where Alice's (Bob's) device has a remote mode a (b) which is maximally entangled with A (B). We then study the separability properties of the global system composed by a, b, A' and B'. In the Markovian case ($\mathbf{G} = \mathbf{0}$), all forms of entanglement (bipartite, tripartite[44], and quadripartite[45]) are absent for $\omega > \omega_{\mathrm{EB}}(\tau) := (1 + \tau)/(1 - \tau)$, so that no protocol can work. In the non-Markovian case ($\mathbf{G} \neq \mathbf{0}$) the presence of separable correlations does not restore bipartite or tripartite entanglement when $\omega > \omega_{\mathrm{EB}}(\tau)$. However, a sufficient amount of these correlations is able to reactivate 1×3 quadripartite entanglement[45], in particular, between mode a and the set of modes $bA'B'$. See Fig. 2.

Once quadripartite entanglement is available, the Bell detection on modes A' and B' can localize it into a bipartite form for modes a and b. For this reason, entanglement swapping and the other protocols can be reactivated by sufficiently-strong separable correlations. In the following, we discuss these results in detail for each specific protocol, starting from the basic scheme of entanglement swapping. For each protocol, we first generalize the theory to non-Markovian decoherence, showing how the various performances are connected. Then, we analyse the protocols under entanglement-breaking conditions.

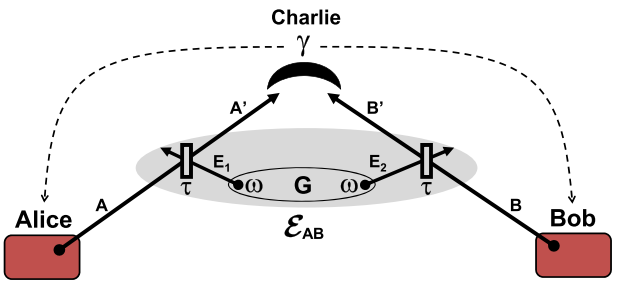

Fig. 1 Quantum relay. Alice and Bob connect their devices (red boxes) to a quantum relay, Charlie, for implementing a CV protocol. On the received modes, Charlie always performs a CV Bell detection whose outcome γ is broadcast. *Separable Gaussian environment*. The travelling modes are subject to a joint Gaussian channel $\mathcal{E}_{AB}$. This is realized by two beam splitters with tranmissivity τ which mix A and B with two ancillary modes, E_1 and E_2, respectively. These ancillas inject thermal noise with variance ω and belong to a correlated (but separable) Gaussian state $\rho_{E_1E_2}$. *Entanglement breaking*. For $\omega > \omega_{\mathrm{EB}}(\tau)$, bipartite (and tripartite) entanglement cannot survive at the relay. In particular, A' is disentangled from Alice's device, and B' is disentangled from Bob's, no matter if the environment is correlated or not. *Non-Markovian reactivation*. Above a critical amount of separable correlations, quadripartite entanglement is reactivated between Alice's and Bob's devices and the transmitted modes, A' and B'. Bell detection can localize this multipartite resource into a bipartite form and reactivate all the protocols.

Entanglement swapping

The standard source of Gaussian entanglement is the two-mode squeezed vacuum (TMSV) state, which is a realistic finite-energy version of the ideal EPR state[10]. More precisely, this is a two-mode

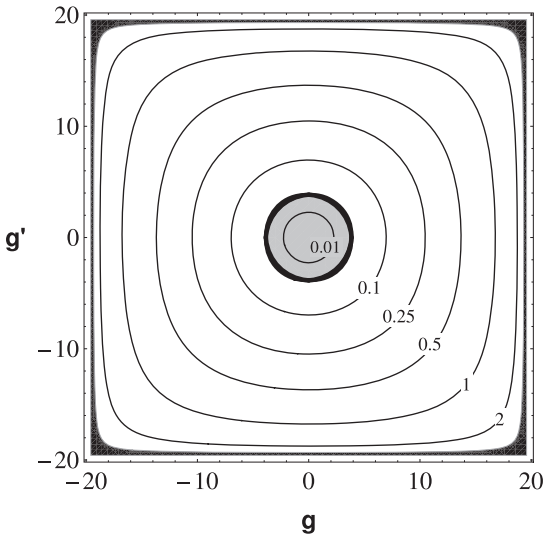

Fig. 2 Non-Markovian reactivation of 1×3 quadripartite entanglement. Assuming maximally entangled states for the parties and entanglement-breaking conditions (here $\tau = 0.9$ and $\omega = 1.02 \times \omega_{\mathrm{EB}} = 19.38$), we show how quadripartite entanglement is reactivated by increasing the separable correlations of the environment (bits of quantum mutual information, which are constant over the concentric contour lines). Inside the grey region there is no quadripartite entanglement with respect to any 1×3 grouping of the four modes $abA'B'$. Outside the grey region all the possible 1×3 groupings are entangled. The external black region is excluded, as it corresponds to entangled or unphysical environments.

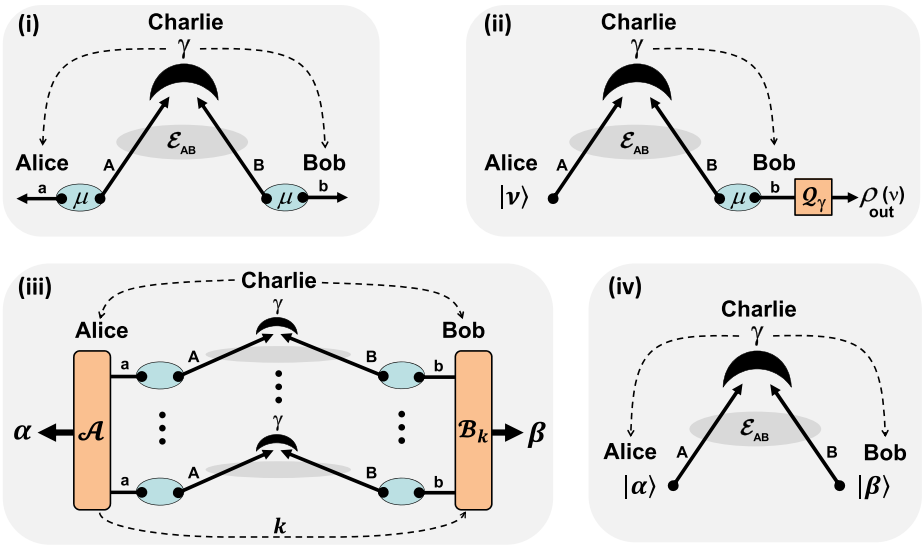

Fig. 3 Relay-based quantum protocols in a correlated Gaussian environment. i *Entanglement swapping*. Alice and Bob possess two TMSV states with variance μ. Modes A and B are sent through the joint channel $\mathcal{E}_{AB}$ and received by Charlie. After the outcome γ is broadcast, the remote modes, a and b, are projected into a conditional state $\rho_{ab|\gamma}$. **ii** *Quantum teleportation*. Alice's coherent state $|\nu\rangle$ is teleported into Bob's state $\rho_{\text{out}}(\nu)$, after the communication of γ and the action of a conditional quantum operation $\mathcal{Q}_\gamma$. **iii** *Entanglement/key distillation*. In the limit of many uses of the relay, Alice performs a quantum instrument on her modes a, communicating a classical variable k to Bob, who performs a conditional quantum operation on his modes b. This is a non-Gaussian quantum repeater where entanglement swapping is followed by optimal one-way distillation. **iv** *Practical QKD*. Alice and Bob prepare Gaussian-modulated coherent states to be sent to Charlie. The communication of the outcome γ creates remote classical correlations which are used to extract a secret key. Here the role of Charlie could be played by Eve, so that the relay becomes an MDI-QKD node.

Gaussian state with zero mean value and CM

$$\mathbf{V}(\mu)=\begin{pmatrix}\mu\mathbf{I} & \sqrt{\mu^2-1}\mathbf{Z}\\ \sqrt{\mu^2-1}\mathbf{Z} & \mu\mathbf{I}\end{pmatrix},\ \mathbf{Z}:=\text{diag}(1,-1),$$

where the variance $\mu\geq 1$ quantifies its entanglement. Indeed the log-negativity[46–48] is strictly increasing in μ: It is zero for $\mu=1$ and tends to infinity for large μ.

Suppose that Alice and Bob have two identical TMSV states, $\rho_{aA}(\mu)$ describing Alice's modes a and A, and $\rho_{bB}(\mu)$ describing Bob's modes b and B, as in Fig. 3(i). They keep a and b, while sending A and B to Charlie through the joint channel $\mathcal{E}_{AB}$ of the Gaussian environment. After the broadcast of the outcome γ, the remote modes a and b are projected into a conditional Gaussian state $\rho_{ab|\gamma}$, with mean value $\mathbf{x}=\mathbf{x}(\gamma)$ and conditional CM $\mathbf{V}_{ab|\gamma}$. In the Supplementary Material, we compute

$$\mathbf{V}_{ab|\gamma}=\begin{pmatrix}\mathbf{A} & \mathbf{C}\\ \mathbf{C}^{\intercal} & \mathbf{B}\end{pmatrix},\tag{1}$$

where the 2×2 blocks are given by

$$\mathbf{A}=\mathbf{B}=\text{diag}\left[\mu-\frac{\mu^2-1}{2(\mu+\kappa)},\mu-\frac{\mu^2-1}{2(\mu+\kappa')}\right],\tag{2}$$

$$\mathbf{C}=\text{diag}\left[\frac{\mu^2-1}{2(\mu+\kappa)},-\frac{\mu^2-1}{2(\mu+\kappa')}\right],\tag{3}$$

and the κ's contain all the environmental parameters

$$\kappa:=(\tau^{-1}-1)(\omega-g),\ \kappa':=(\tau^{-1}-1)(\omega+g').\tag{4}$$

From $\mathbf{V}_{ab|\gamma}$ we compute the log-negativity $\mathcal{N}=\max\{0,-\log_2\varepsilon\}$ of the swapped state, in terms of the smallest partially transposed symplectic eigenvalue ε[10]. In the Supplementary Material, we derive

$$\varepsilon=\left[\frac{(1+\mu\kappa)(1+\mu\kappa')}{(\mu+\kappa)(\mu+\kappa')}\right]^{1/2}.\tag{5}$$

For any input entanglement ($\mu>1$), swapping is successful ($\varepsilon<1$) whenever the environment has enough correlations to satisfy the condition $\kappa\kappa'<1$. The actual amount of swapped entanglement $\mathcal{N}$ increases in μ, reaching its asymptotic optimum for large μ, where

$$\varepsilon\simeq\varepsilon_{\text{opt}}:=\sqrt{\kappa\kappa'}.$$

Quantum teleportation

As depicted in Fig. 3(ii), we consider Charlie acting as a teleporter of a coherent state $|\nu\rangle$ from Alice to Bob. Alice's state and part of Bob's TMSV state are transmitted to Charlie through the joint channel $\mathcal{E}_{AB}$. After detection, the outcome γ is communicated to Bob, who performs a conditional quantum operation[2] $\mathcal{Q}_\gamma$ on mode b to retrieve the teleported state $\rho_{\text{out}}(\nu)\simeq|\nu\rangle\langle\nu|$. In the Supplementary Material, we find a formula for the teleportation fidelity $F=F(\mu,\kappa,\kappa')$, which becomes asymptotically optimal for large μ, where

$$F\simeq F_{\text{opt}}:=[(1+\kappa)(1+\kappa')]^{-1/2}\leq(1+\varepsilon_{\text{opt}})^{-1}.\tag{6}$$

Thus, there is a direct connection between the asymptotic protocols of teleportation and swapping: If swapping fails ($\varepsilon_{\text{opt}}\geq 1$), teleportation is classical ($F_{\text{opt}}\leq 1/2$ (ref. [10])). We retrieve the relation $F_{\text{opt}}=(1+\varepsilon_{\text{opt}})^{-1}$ in environments with antisymmetric correlations $g+g'=0$.

Entanglement distillation

Entanglement distillation can be operated on top of entanglement swapping as depicted in Fig. 3(iii). After the parties have run the swapping protocol many times and stored their remote modes in quantum memories, they can perform a one-way entanglement distillation protocol on the whole set of swapped states $\rho_{ab|\gamma}$. This consists of Alice locally applying an optimal quantum instrument[49] $\mathcal{A}$ on her modes a, whose quantum outcome $\boldsymbol{\alpha}$ is a distilled system while the classical outcome k is communicated. Upon

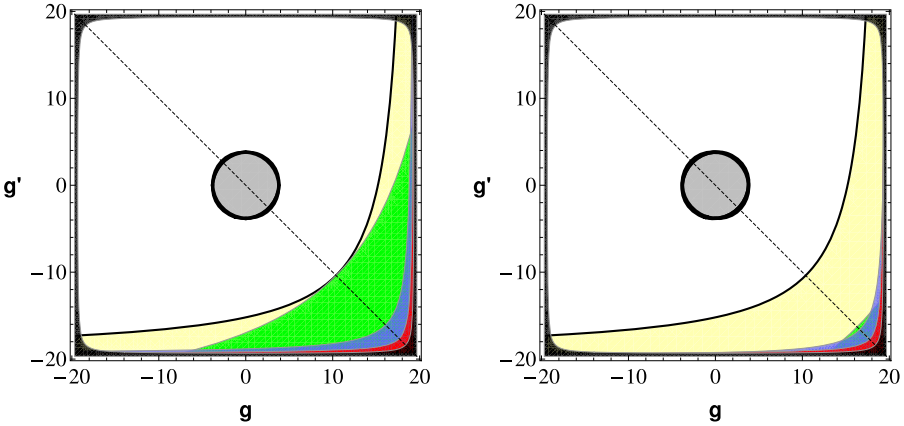

Fig. 4 Non-Markovian reactivation of quantum protocols from entanglement-breaking (here $\tau = 0.9$ and $\omega = 1.02 \times \omega_{EB} = 19.38$). Each point of the correlation plane corresponds to a Gaussian environment with separable correlations. In the left panel we consider the optimal scenario of large μ (asymptotic protocols). Once quadripartite 1×3 entanglement has been reactivated (outside the grey ring), we have the progressive reactivation of entanglement swapping ($\mathcal{N} > 0$, yellow region), quantum teleportation of coherent states ($F > 1/2$, green region), entanglement/key distillation ($I_{\mathcal{C}}$, $K > 0$, blue region) and practical QKD ($R > 0$, red region). The right panel refers to a realistic scenario with experimentally achievable values of μ. We consider $\mu \simeq 6.5$ (refs. [54,55]) as input entanglement for the entanglement-based protocols, and $\mu \simeq 50$ as modulation for the practical QKD protocol. The reactivation phenomenon persists and can be explored with current technology. Apart from teleportation, the other thresholds undergo small modifications.

receipt of k, Bob performs a conditional quantum operation $\mathcal{B}_k$ transforming his modes b into a distilled system β.

The process can be designed in such a way that the distilled systems are collapsed into entanglement bits (ebits), i.e., Bell state pairs[2]. The optimal distillation rate (ebits per relay use) is lower-bounded[49] by the coherent information $I_{\mathcal{C}}$[50,51] computed on the single copy state $\rho_{ab|\gamma}$. In the Supplementary Material, we find a closed expression $I_{\mathcal{C}} = I_{\mathcal{C}}(\mu, \kappa, \kappa')$ which is maximized for large μ, where $I_{\mathcal{C}} \simeq -\log_2(e\varepsilon_{\text{opt}})$. Asymptotically, entanglement can be distilled for $\varepsilon_{\text{opt}} < e^{-1} \simeq 0.367$.

Secret-key distillation

The scheme of Fig. 3(iii) can be modified into a key distillation protocol, where Charlie (or Eve[22]) distributes secret correlations to Alice and Bob, while the environment is the effect of a Gaussian attack. Alice's quantum instrument is here a measurement with classical outputs $\boldsymbol{\alpha}$ (the secret key) and k (data for Bob). Bob's operation is a measurement conditioned on k, which provides the classical output $\boldsymbol{\beta}$ (key estimate). This is an ideal key-distribution protocol[52] whose rate is lower-bounded by the coherent information, i.e., $K \geq I_{\mathcal{C}}$ (see Supplementary Material).

Practical QKD

The previous key-distribution protocol can be simplified by removing quantum memories and using single-mode measurements, in particular, heterodyne detections. This is equivalent to a run-by-run preparation of coherent states, $|\alpha\rangle$ on Alice's mode A, and $|\beta\rangle$ on Bob's mode B, whose amplitudes are Gaussianly modulated with variance $\mu - 1$. As shown in Fig. 3(iv), these states are transmitted to Charlie (or Eve[22]) who measures and broadcasts $\gamma \simeq \alpha - \beta^*$.

Assuming ideal reconciliation[10], the secret key rate $R = R(\mu, \kappa, \kappa')$ increases in μ. Modulation variances $\mu \gtrsim 50$ are experimentally achievable and well approximate the asymptotic limit for $\mu \gg 1$, where the key rate is optimal and satisfies (see Supplementary Material)

$$R_{\text{opt}} \gtrsim \log_2\left(\frac{F_{\text{opt}}}{e^2\varepsilon_{\text{opt}}}\right) + h(1 + 2\varepsilon_{\text{opt}}), \tag{7}$$

with $h(x) := \frac{x+1}{2}\log_2\frac{x+1}{2} - \frac{x-1}{2}\log_2\frac{x-1}{2}$. Using Eq. (6), we see that the right-hand side of Eq. (7) can be positive only for $\varepsilon_{\text{opt}} \lesssim 0.192$.

Thus the practical QKD protocol is the most difficult to reactivate: Its reactivation implies that of entanglement/key distillation and that of entanglement swapping. This is true not only asymptotically but also at finite μ as we show below.

Reactivation from entanglement breaking

Once the theory of the previous protocols has been extended to non-Markovian decoherence, we can study their reactivation from entanglement-breaking conditions. Consider an environment with transmissivity τ and entanglement-breaking thermal noise $\omega > \omega_{\text{EB}}(\tau)$, so that no protocol can work for $\mathbf{G} = \mathbf{0}$. By increasing the separable correlations in the environment, not only can quadripartite entanglement be reactivated but, above a certain threshold, it can also be localized into a bipartite form by the relay's Bell detection. Once entanglement swapping is reactivated, all other protocols can progressively be reactivated. As shown in Fig. 4, there are regions of the correlation plane where entanglement can be swapped ($\mathcal{N} > 0$), teleportation is quantum ($F > 1/2$), entanglement and keys can be distilled ($I_{\mathcal{C}}$, $K > 0$), and practical QKD can be performed ($R > 0$). This occurs both for large and experimentally achievable values of μ.

Note that the reactivation is asymmetric in the plane only because of the specific Bell detection adopted, which generates correlations of the type $g > 0$ and $g' < 0$. Using another Bell detection (projecting onto $\hat{q}_+$ and $\hat{p}_-$), the performances would be inverted with respect to the origin of the plane. Furthermore, the entanglement localization (i.e., the reactivation of entanglement swapping) is triggered for correlations higher than those required for restoring quadripartite entanglement, suggesting that there might exist a better quantum measurement for this task. The performances of the various protocols improve by increasing the separable correlations of the environment, with the fastest reactivation being achieved along the diagonal $g + g' = 0$, where swapping and teleportation are first recovered, then entanglement/key distillation and practical QKD, which is the most nested region.

Correlated additive noise

The phenomenon can also be found in other types of non-Markovian Gaussian environments. Consider the limit for $\tau \to 1$ and $\omega \to +\infty$, while keeping constant $n := (1 - \tau)\omega$, $c := g(\omega - 1)^{-1}$

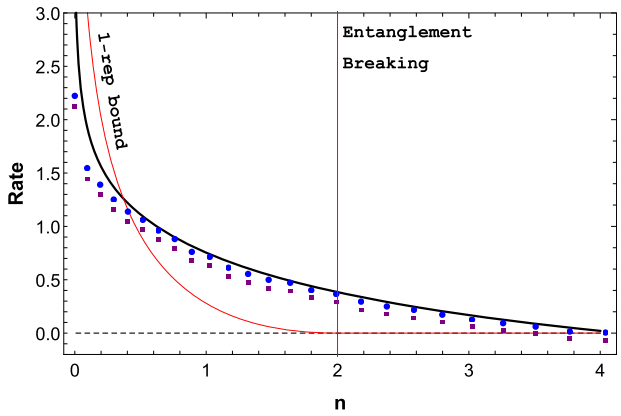

Fig. 5 Plot the secret-key rate *R* (bits per relay use) as a function of the additive noise *n*. The solid black curve is the theoretical rate computed for a correlated additive environment ($c = c' = 1$) and realistic signal modulation ($\mu \simeq 52$). This rate is positive after entanglement breaking ($n > 2$) and beats the single-repeater bound[40] (based on memoryless links). Points are experimental data: blue circles refer to ideal reconciliation and purple squares to achievable reconcilation efficiency (≃0.97). Error bars on the *x*-axis are smaller than the point size. Due to loss at the untrusted relay, the experimental key rate is slightly below the theoretical curve (associated with the correlated side-channel attack).

and $c' := g'(\omega - 1)^{-1}$. This is an asymptotic environment which adds correlated classical noise to modes *A* and *B*, so that their quadratures undergo the transformations

$$(\hat{q}_A, \hat{p}_A, \hat{q}_B, \hat{p}_B) \rightarrow (\hat{q}_A, \hat{p}_A, \hat{q}_B, \hat{p}_B) + (\xi_1, \xi_2, \xi_3, \xi_4).$$

Here the ξ_i's are zero-mean Gaussian variables whose covariances $\langle \xi_i \xi_j \rangle$ are specified by the classical CM

$$\mathbf{V}(n, c, c') = n(\mathbf{I}\mathrm{diag}(c, c')\mathrm{diag}(c, c')\mathbf{I}), \quad (8)$$

where $n \geq 0$ is the variance of the additive noise, and $-1 \leq c, c' \leq 1$ quantify the classical correlations. The entanglement-breaking condition becomes $n > 2$.

To show non-Markovian effects, we consider the protocol which is the most difficult to reactivate, the practical QKD protocol. We can specify its key rate $R(\mu, n, c, c')$ for $c = c' = 1$ and assume a realistic modulation $\mu \simeq 52$. We then plot *R* as a function of the additive noise *n* in Fig. 5. As we can see, the rate decreases in *n* but remains positive in the region $2 < n \leq 4$ where the links with the relay become entanglement-breaking. As we show below, this behaviour persists in the presence of loss, as typically introduced by experimental imperfections.

Recall that, for an additive Gaussian channel with added noise *n*, the secret-key capacity (and any other two-way assisted quantum capacity) is upper-bounded by

$$\Phi(n) := \frac{(n/2) - 1}{\ln 2} - \log_2(n/2), \quad (9)$$

for $n \leq 2$ and zero otherwise. The bound $\Phi(n)$ in Eq. (9) has been proven in ref. [53] [see Eq. (29)] and here reported in our different vacuum units. In the presence of a relay/repeater, where each link is described by an independent bosonic Gaussian channel, ref. [40] established that the secret-key capacity assisted by the repeater $K_{1-\mathrm{rep}}$ is upper-bounded by the minimum secret-key capacity of the links. In the present setting, we therefore have the single-repeater bound $K_{1-\mathrm{rep}} \leq \Phi(n)$. As we show in Fig. 5, the presence of classical (separable) correlations in the Gaussian environment lead to the violation of the bound $\Phi(n)$ when $n \gtrsim 0.369$ (for the theoretical curve) and $n \gtrsim 0.4$ (for the experimental results).

Experimental results

Our theoretical results are confirmed by a proof-of-principle experiment, whose setup is schematically depicted in Fig. 6. We consider Alice and Bob generating Gaussianly modulated coherent states by means of independent electro-optical modulators, applied to a common local oscillator. Simultaneously, the modulators are subject to a side-channel attack: Additional electrical inputs are introduced by Eve, whose effect is to generate additional and unknown phase-space displacements. In particular, Eve's electrical inputs are correlated so that the resulting optical displacements introduce a correlated additive Gaussian environment described by Eq. (8) with $c \simeq 1$ and $c' \simeq 1$. The optical modes then reach the midway relay, where they are mixed at a balanced beam splitter and the output ports photo-detected. Although the measurement is highly efficient, it introduces a small loss (≃2%) which is assumed to be exploited by Eve in the worst-case scenario.

From the point of view of Alice and Bob, the side-channel attack and the additional (small) loss at the relay are jointly perceived as a global coherent Gaussian attack of the optical modes. Analysing the statistics of the shared classical data and assuming that Eve controls the entire environmental purification compatible with this data, the two parties may compute the experimental secret-key rate (see details in the Supplementary Material). As we can see from Fig. 5, the experimental points are slightly below the theoretical curve associated with the correlated additive environment, reflecting the fact that the additional loss at the relay tends to degrade the performance of the protocol. The experimental rate is able to beat the single-repeater bound for additive-noise Gaussian links[40] and remains positive after the entanglement-breaking threshold, so that the non-Markovian reactivation of QKD is experimentally confirmed.

DISCUSSION

We have theoretically and experimentally demonstrated that the most important protocols operated by quantum relays can work in conditions of extreme decoherence thanks to the presence of non-Markovian memory effects in the environment. Assuming high Gaussian noise in the links, we have considered a regime where any form of entanglement (bipartite, tripartite, or quadripartite) is broken under Markovian memoryless conditions. By allowing for a suitable amount of correlations in the environment, we have proven that we can reactivate the distribution of 1×3 quadripartite entanglement, and this resource can successfully be localized into a bipartite form exploitable by Alice and Bob. As a result, all the basic protocols for quantum and private communication can be progressively reactivated by the action of the relay.

Surprisingly, this reactivation is possible without the need of any injection of entanglement from the environment, but just because of the presence of weaker classical correlations (described by a separable state for the environment). In particular, we have shown that these correlations lead to the violation of the single-repeater bound for quantum and private communications.

Our results might open new perspectives for all quantum systems where correlated errors and memory effects are typical forms of decoherence. This may involve both short-distance implementations (e.g., chip-based) and long-distance ones, as is the case of relay-based QKD. Non-Markovian memory effects should therefore be regarded as a potential physical resource to be exploited in various settings of quantum communication.

METHODS

Theoretical and experimental methods are given in the Supplementary Material. Theoretical methods contain details about the following points: (i)

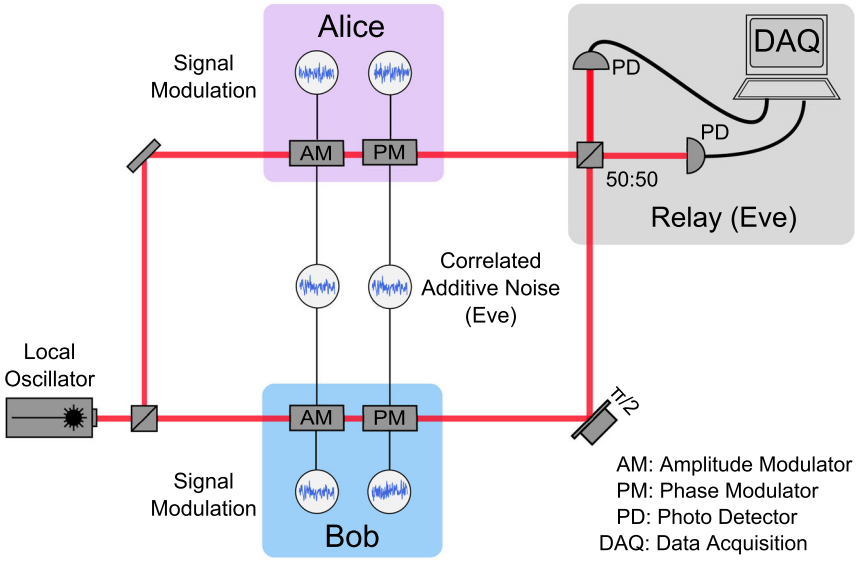

Fig. 6 Experimental setup. Alice and Bob receive 1064 nm light from the same laser source (local oscillator). At both stations, the incoming beams are Gaussianly modulated in phase and amplitude using electro-optical modulators driven by uncorrelated signal generators. In addition, the phase and amplitude modulators for Alice and Bob have correlated inputs respectively, such that a noisy modulation identical for both Alice and Bob is added to the phase and amplitude signals (side-channel attack). The magnitudes of the correlated noise modulations are progressively increased (from $n = 0$ to 4), and kept symmetrical between the quadratures, while the signal modulations are kept constant at the same level in both quadratures for Alice and Bob ($\mu \simeq 52$). At the untrusted relay, the modes are mixed at a balanced beam splitter and the output ports photo-detected, with an overall efficiency of ≃98%. Photocurrents are then processed to realize a CV Bell measurement. See Supplementary Material for details.

Study of the Gaussian environment with correlated thermal noise, including a full analysis of its correlations. (ii) Study of the various forms of entanglement available before the Bell detection of the relay. (iii) Study of the entanglement swapping protocol, i.e., the computation of the CM $\mathbf{V}_{ab|\gamma}$ in Eq. (1) and the derivation of the eigenvalue ε in Eq. (5). (iv) Generalization of the teleportation protocol with details on Bob's quantum operation $\mathcal{Q}_\gamma$ and the analytical formula for the fidelity $F(\mu,\kappa,\kappa')$. (v) Details of the distillation protocol with the analytical formula of $I_{\mathcal{C}}(\mu,\kappa,\kappa')$. (vi) Details of the ideal key-distillation protocol, discussion on MDI-security, and proof of the lower-bound $K \geq I_{\mathcal{C}}$. (vii) Derivation of the general secret-key rate $R(\xi,\mu,\kappa,\kappa')$ of the practical QKD protocol, assuming arbitrary reconciliation efficiency ξ and modulation variance μ. (viii) Explicit derivation of the optimal rate R_{opt} and the proof of the tight lower bound in Eq. (7). (ix) Derivation of the correlated additive environment as a limit of the correlated thermal one. (x) Study of entanglement swapping and practical QKD in the correlated additive environment, providing the formula of the secret-key rate $R(\xi,\mu,n,c,c')$.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Received: 12 April 2020; Accepted: 17 April 2021;
Published online: 21 May 2021

REFERENCES

1. Cover, T. M. & Thomas, J. A. *Elements of Information Theory* 2nd edn (Wiley, 2006).
2. Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).
3. Bouwmeester, D. *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation* (Springer, 2000).
4. Vedral, V. *Introduction to Quantum Information Science* (Oxford University Press, 2006).
5. Bengtsson, I. & Życzkowski, K. *Geometry of Quantum States: An Introduction to Quantum Entanglement* (Cambridge University Press, 2006).
6. Barnett, S. *Quantum Information* (Oxford University Press, 2009).
7. Schumacher, B. & Westmoreland, M. *Quantum Processes Systems, and Information* (Cambridge University Press, 2010).
8. Holevo, A. *Quantum Systems, Channels, Information: A Mathematical Introduction* (De Gruyter, 2012).
9. Watrous, J. *The Theory of Quantum Information* (Cambridge University Press, 2018).
10. Weedbrook, C. et al. Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621 (2012).
11. Braunstein, S. L. & van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* **77**, 513 (2005).
12. Andersen, U. L., Neergaard-Nielsen, J. S., van Loock, P. & Furusawa, A. Hybrid quantum information processing. *Nat. Phys.* **11**, 713–719 (2015).
13. Kurizki, G. et al. Quantum technologies with hybrid systems. *Proc. Natl. Acad. Sci. USA* **112**, 3866–73 (2015).
14. Zukowski, M., Zeilinger, A., Horne, M. A. & Ekert, A. "Event ready detectors" Bell experiment via entanglement swapping. *Phys. Rev. Lett.* **71**, 4287 (1993).
15. van Loock, P. & Braunstein, S. L. Unconditional teleportation of continuous-variable entanglement. *Phys. Rev. A* **61**, 010302(R) (1999).
16. Polkinghorne, R. E. S. & Ralph, T. C. Continuous variable entanglement swapping. *Phys. Rev. Lett.* **83**, 2095 (1999).
17. Pirandola, S., Vitali, D., Tombesi, P. & Lloyd, S. Macroscopic entanglement by entanglement swapping. *Phys. Rev. Lett.* **97**, 150403 (2006).
18. Briegel, H.-J., Dür, W., Cirac, J. I. & Zoller, P. Quantum repeaters: the role of imperfect local operations in quantum communication. *Phys. Rev. Lett.* **81**, 5932 (1998).
19. Bennett, C. H. et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70**, 1895 (1993).
20. Furusawa, A. et al. Unconditional quantum teleportation. *Science* **282**, 706 (1998).
21. Pirandola, S., Eisert, J., Weedbrook, C., Furusawa, A. & Braunstein, S. L. Advances in quantum teleportation. *Nat. Photonics* **9**, 641–652 (2015).
22. Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012).
23. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
24. Pirandola, S. et al. High-rate measurement-device-independent quantum cryptography. *Nat. Photonics* **9**, 397–402 (2015).
25. Lucamarini, M., Yuan, Z. L., Dynes, J. F. & Shields, A. J. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400 (2018).
26. Wang, X.-B., Yu, Z.-W. & Hu, X.-L. Twin-field quantum key distribution with large misalignment error. *Phys. Rev. A* **98**, 062323 (2018).

27. Pirandola, S. et al. Advances in quantum cryptography. *Adv. Opt. Photon.* **12**, 1012–1236 (2020).
28. Metcalf, B. J. et al. Quantum teleportation on a photonic chip. *Nat. Photonics* **8**, 770–774 (2014).
29. Masada, G. et al. Continuous-variable entanglement on a chip. *Nat. Photonics* **9**, 316–319 (2015).
30. L. Steffen, L. et al. Deterministic quantum teleportation with feed-forward in a solid state system. *Nature* **500**, 319 (2013).
31. Breuer, H.-P. & Petruccione, F. *The Theory of Open Quantum Systems* (Oxford University Press, 2002).
32. Lassen, M., Berni, A., Madsen, L. S., Filip, R. & Andersen, U. L. Gaussian error correction of quantum states in a correlated noisy channel. *Phys. Rev. Lett.* **111**, 180502 (2013).
33. Tyler, G. A. & Boyd, R. W. Influence of atmospheric turbulence on the propagation of quantum states of light carrying orbital angular momentum. *Opt. Lett.* **34**, 142 (2009).
34. Semenov, A. A. & Vogel, W. Quantum light in the turbulent atmosphere. *Phys. Rev. A* **80**, 021802(R) (2009).
35. Boyd, R. W., Rodenburg, B., Mirhosseini, M. & Barnett, S. M. Influence of atmospheric turbulence on the propagation of quantum states of light using plane-wave encoding. *Opt. Express* **19**, 18310 (2011).
36. Renner, R. Symmetry of large physical systems implies independence of subsystems. *Nat. Phys.* **3**, 645–649 (2007).
37. Renner, R. & Cirac, J. I. de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Phys. Rev. Lett.* **102**, 110504 (2009).
38. Horodecki, M., Shor, P. W. & Ruskai, M. B. General entanglement breaking channels. *Rev. Math. Phys.* **15**, 629 (2003).
39. Holevo, A. S. Entanglement-breaking channels in infinite dimensions. *Probl. Inform. Transm.* **44**, 3 (2008).
40. Pirandola, S. End-to-end capacities of a quantum communication network. *Commun. Phys.* **2**, 51 (2019) [Preprint at arXiv:1601.00966 (2016)].
41. Spedalieri, G., Ottaviani, C. & Pirandola, S. Covariance matrices under Bell-like detections. *Open Syst. Inf. Dyn.* **20**, 1350011 (2013).
42. Pirandola, S., Serafini, A. & Lloyd, S. Correlation matrices of two-mode bosonic systems. *Phys. Rev. A* **79**, 052327 (2009).
43. Pirandola, S. Entanglement reactivation in separable environments. *New J. Phys.* **15**, 113046 (2013).
44. Giedke, G., Kraus, B., Lewenstein, M. & Cirac, J. I. Separability properties of three-mode Gaussian states. *Phys. Rev. A* **64**, 052303 (2001).
45. Werner, R. F. & Wolf, M. M. Bound entangled Gaussian states. *Phys. Rev. Lett.* **86**, 3658 (2001).
46. Vidal, G. & Werner, R. F. Computable measure of entanglement. *Phys. Rev. A* **65**, 032314 (2002).
47. Eisert, J. *Entanglement in Quantum Information Theory*. Ph.D. thesis (Potsdam, February 2001).
48. Plenio, M. B. The logarithmic negativity: a full entanglement monotone that is not convex. *Phys. Rev. Lett.* **95**, 090503 (2005).
49. Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. Lond. A* **461**, 207 (2005).
50. Schumacher, B. & Nielsen, M. A. Quantum data processing and error correction. *Phys. Rev. A* **54**, 2629 (1996).
51. Lloyd, S. Capacity of the noisy quantum channel. *Phys. Rev. A* **55**, 1613 (1997).
52. Pirandola, S., García-Patrón, R., Braunstein, S. L. & Lloyd, S. Direct and reverse secret-key capacities of a quantum channel. *Phys. Rev. Lett.* **102**, 050503 (2009).
53. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017).
54. Eckstein, A., Christ, A., Mosley, P. J. & Silberhorn, C. Highly efficient single-pass source of pulsed single-mode twin beams of light. *Phys. Rev. Lett.* **106**, 013603 (2011).
55. Eberle, T., Händchen, V. & Schnabel, R. Stable control of 10 dB two-mode squeezed vacuum states of light. *Opt. Express* **21**, 11546 (2013).

ACKNOWLEDGEMENTS

This work has been funded by the EPSRC via the projects 'qDATA' (EP/L011298/1) and 'Quantum Communications hub' (EP/M013472/1, EP/T001011/1), and by the European Union via 'Continuous Variable Quantum Communications' (CiViQ, grant agreement No 820466). S.P. also thanks the Leverhulme Trust (research fellowship 'qBIO'). G.S. has been sponsored by the EU via a Marie Skłodowska-Curie Global Fellowship (grant No. 745727). T.G. acknowledges support from the H. C. Ørsted postdoc programme. U.L.A. thanks the Danish Agency for Science, Technology and Innovation (Sapere Aude project).

AUTHOR CONTRIBUTIONS

S.P. developed the theory, with contributions from C.O., G.S. and S.L.B. C.S.J. performed the experiment. T.G. and U.L.A. supervised the experiment. S.P. wrote the manuscript with the experimental part being edited by U.L.A. All authors were involved in technical discussions.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-021-00413-2.

Correspondence and requests for materials should be addressed to S.P.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.